Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Érico Asano de Mello

RÁDIO COGNITIVO:

Aspectos de segurança

Rio de Janeiro

2010

Érico Asano de Mello

RÁDIO COGNITIVO:

Aspectos de segurança

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Campos Cruz, M.Sc., UFRJ, Brasil

Rio de Janeiro

2010

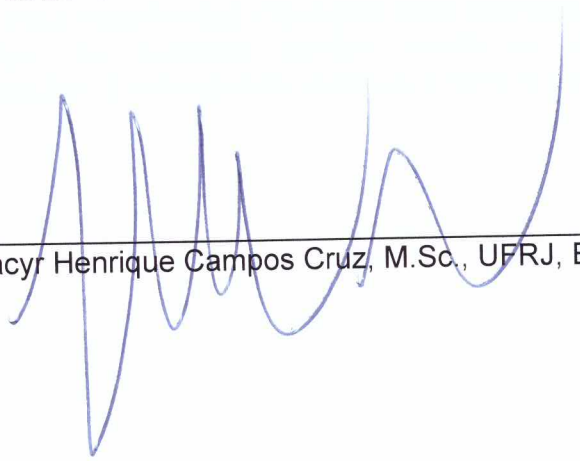
Érico Asano de Mello

RÁDIO COGNITIVO:

Aspectos de segurança

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2010.



Moacyr Henrique Campos Cruz, M.Sc., UFRJ, Brasil

Dedico esse trabalho aos meus pais pelo incentivo, cooperação e apoio para que eu pudesse concluir todos os meus estudos sem preocupações e perseguisse os meus objetivos até o fim.

AGRADECIMENTOS

Meus sinceros agradecimentos a todos aqueles que de alguma forma doaram um pouco de si para que a conclusão deste trabalho se tornasse possível:

Aos meus pais, pelo incentivo e carinho.

Ao meu orientador Moacyr Henrique por ter se preocupado e incentivado a continuar o projeto de pesquisa.

À minha irmã, pela amizade e companhia.

RESUMO

Mello, Érico Asano de. **RÁDIO COGNITIVO: Aspectos de Segurança**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

Este trabalho descreve como Redes de Rádios Cognitivos estão se tornando parte muito importante da tecnologia wireless, devido à escassez do espectro de frequência livre de interferência. Rádio cognitivo tem por concepção operar oportunisticamente em faixas de frequência licenciadas, sem causar interferência em usuários primários. Contudo, assim como em várias outras tecnologias, os aspectos de segurança não são o foco principal. O paradigma do rádio cognitivo introduz várias novas classes de ameaças de segurança e novos desafios, sendo mais difícil prover alta segurança, quando comparado com redes sem fio tradicionais.

Dispositivos wireless que têm capacidade de aprendizado de acordo com o seu ambiente podem também ser ensinados por elementos maliciosos. Como a tabela de estados do rádio cognitivo é composta com fatos aprendidos do passado e medições atuais do sensor, o comportamento futuro do dispositivo pode ser modificado apenas manipulando os dados de entrada do sensor.

Ainda nesse trabalho são apresentados os maiores desafios para prover segurança em redes cognitivas; é apresentado o padrão de rádio cognitivo IEEE 802.22, e são identificadas as potenciais ameaças junto com abordagens de mitigação.

ABSTRACT

Mello, Érico Asano de. **RÁDIO COGNITIVO: Aspectos de Segurança**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

The present work describes how Cognitive Radio Networks are becoming a very important part of the wireless technology, due to the scarcity of spectrum resources. Cognitive radio is expected to operate in licensed frequency band opportunistically without cause interference to licensed or primary users. As many other new techniques, the security factors are out of focus. The cognitive radio paradigm introduces entirely new classes of security threats and challenges, and providing strong security may be difficult when compared with traditional wireless networks.

Wireless devices that can learn from their environment can also to be taught be malicious elements. As the state space for a cognitive radio is made up for a variety of learned beliefs and current sensor inputs, we can modify future behavior of the device just manipulating radio sensor inputs.

This work presents the key challenges in providing security in cognitive networks, discusses the emerging IEEE 802.22 cognitive radio standard, and identifies potentials threats along with potential mitigation approaches.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

BS	Estação Base (Base Station)
CCS	Cabeçalho de controle do Superframe
DoS	Negação de Serviço (Denial of Service)
FCC	Federal Communication Comission
FCL	Lista de Canais Livres (Free Channel List)
PDU	Protocol Data Unit
PUE	Emulação do Usuário Primário (Primary User Emulation)
RAN	Regional Area Network
RC	Radio Cognitivo

SUMÁRIO

1 INTRODUÇÃO

A alta demanda por serviços de rede sem fio com alta disponibilidade de banda tem impulsionado as indústrias de comunicação e, de fato, percebe-se um grande avanço nas tecnologias wireless no que diz respeito aos serviços disponibilizados ou às capacidades dos canais de comunicação.

O aumento das velocidades de transmissão, contudo, está diretamente relacionado à disponibilidade de um espectro de frequência livre de interferência. Devido à imensa quantidade de dispositivos wireless, esse recurso (o espectro), tem se tornado uma limitação e tem como principal causa o mau gerenciamento do espectro. Agências reguladoras alocam faixas de frequência para serviços específicos, que são normalmente estáticas, o que significa que estarão indisponíveis para uso, mesmo que quem tenha o direito de utilizar não a esteja usando no momento.

A alocação de bandas de frequência para uso não licenciado permitiu o crescimento da tecnologia 802.11, porém essas faixas já começam a ficar superpopuladas.

A FCC (Federal Comunications Commission) visando solucionar o problema, trabalha no desenvolvimento de novas políticas de gerenciamento de espectros de frequência e, desde o início de 2009, adotou a medida de liberar o acesso oportunista a canais das bandas VHF e UHF [1]. Rádios não licenciados podem utilizar os canais de uma faixa de espectro sem atividade de sistemas licenciados, desde que tenham a capacidade de se adaptar para evitar interferência, caso um rádio licenciado comece a transmitir.

Radio cognitivo (RC) é uma tecnologia que busca utilizar eficientemente o espectro de frequência, podendo ser definido como um sistema de rádio que sente o

seu ambiente operacional eletromagnético e pode ajustar dinamicamente seus parâmetros de operação, maximizando o *throughput*.

Utilizando-se de métodos de consulta a banco de dados centralizados ou medições do meio, os rádios cognitivos são capazes de detectar a presença de outros rádios e se adaptar para evitar prejudicar o funcionamento de rádios licenciados, também chamados de primários.

O IEEE 802.22 foi o primeiro padrão de larga escala desenvolvido para utilizar o espectro reservado para TV e microfone wireless para serviços de banda larga. O desafio do protocolo é prover proteção dos usuários primários desse espectro.

O 802.22 sofreu influência do 802.16e no que diz respeito ao modelo e mecanismos de segurança, porém, há muitos aspectos específicos a rádios cognitivos (RC) que não são tratados por este último protocolo. 802.16e provê boa segurança contra vários tipos de ataque, contudo RC introduz uma série de novas ameaças, como por exemplo o DoS (Denial of Service), que passa a ser muito mais difícil de ser mitigado.

Semelhante a qualquer rede wireless, deseja-se prover confidencialidade, autenticação, integridade e disponibilidade em redes baseadas em RC, porém esta última apresenta duas diferenças fundamentais em relação a redes sem fio tradicionais: o potencial de um ataque comprometer a rede em grande escala por longo tempo e a possibilidade de um ataque comprometer profundamente o desempenho da rede com uma manipulação simples do espectro. Induzir um RC a perceber o ambiente incorretamente resulta na sua adaptação incorreta e consequentemente afeta o desempenho ou disponibilidade da rede. Além disso, os RC usam a experiência para antecipar ações futuras e também colaboram com rádios vizinhos para propagar o comportamento através da rede, podendo um

atacante manipular o espectro e indisponibilizar uma rede por um longo período e em um longo alcance.

Ao atuar numa determinada faixa de frequência, 802.22 deve “ceder a vez” ao detectar uma interferência de um usuário primário dessa faixa (*licenciado*) e deve achar um novo espectro para operar. No caso de dispositivos específicos, como microfones wireless, é mais fácil garantir a autenticidade do sinal, pois esses equipamentos podem trabalhar com dispositivos especializados 802.22 para sinalizar a presença através de mensagens de sinalização, que podem ser autenticados. Porém, mecanismos para determinar a autenticidade de sinais de TV são mais complexos. A localização dos transmissores de TV deve ser conhecida previamente para determinar limiares de interferência para considerá-la um sinal válido. Mesmo assim um atacante pode ajustar o seu sinal até observar uma adaptação dos RCs e continuar “perseguindo” o novo espectro usado pelo rádio.

As camadas física e de enlace em redes de RC são bem diferentes daquelas em redes sem fio convencionais. Alguns aspectos particulares, como a escuta do espectro em cooperação e mecanismos de coexistência com usuários licenciados e com outros usuários primários, trazem novos desafios de segurança.

Essa pesquisa primeiramente explica o funcionamento do protocolo 802.22 (Rádio Cognitivo), posteriormente abordando as características gerais de RC e de redes de RC, independente da proposta apresentada no 802.22, que já impõe um modo de funcionamento centralizado. A seguir, no capítulo 4, são apresentadas as vulnerabilidades e ameaças a que os RC estão sujeitos finalizando no capítulo 5 com mecanismos de mitigação dessas ameaças.

2 VISÃO GERAL DO PROTOCOLO IEEE 802.22

O grupo de Trabalho 802.22 foi criado em 2004 para tratar o uso de rádios não licenciados operando na banda reservada à transmissão de TV, sem causar prejuízo às suas transmissões, e focando nas camadas PHY e MAC desse protocolo de comunicação baseado em rádio cognitivo.

802.22 foi criado a princípio tendo como alvo o uso em áreas rurais e remotas, em que a disponibilidade do acesso banda larga torna-se mais crítica. A banda de TV foi escolhida para prover o serviço por apresentar características de propagação favoráveis, sendo capaz de atingir usuários mais distantes, e também por ser observado que esse espectro estava sendo pouco ocupado. O protocolo também foi concebido para atuar no escopo de frequência dos microfones wireless.

O funcionamento do protocolo consiste basicamente em identificar dinamicamente e usar porções do espectro que estão livres. Contudo, caso a disponibilidade desse espectro venha a ser alterada por algum outro rádio licenciado, o RC deve se adaptar rapidamente para não prejudicar as transmissões licenciadas.

Deve ser mencionado que o IEEE 802.22 é focado nas camadas mais baixas da pilha de protocolos e grande parte dos estudos é realizada para mitigar a interferência, provendo para isso, agilidade do protocolo para mudar de frequência de operação.

Como requisito para garantir a detecção e proteção das transmissões dos usuários primários, a especificação do 802.22 provê diversos mecanismos como: escuta distribuída do espectro; períodos para gerenciamento do processo de escuta; algoritmos de detecção e de medição, e gerenciamento do espectro.

Para manter o conhecimento do ambiente espectral, rádios cognitivos 802.22 utilizam dois métodos: um banco de dados de localização geográfica de dispositivos e escuta do espectro. No primeiro método, o conhecimento da localização de transmissores licenciados pode ser utilizada para determinar que canais estão disponíveis para uso num determinado local. Um banco de dados com a localização dos transmissores de TV proporciona vantagens para o protocolo 802.22, porém, no caso de transmissores de baixa potência (ex. microfone wireless) há um desafio maior no processo de detecção. Esses dispositivos podem surgir em qualquer lugar e em grande quantidade. No segundo método, é possível identificar em tempo real quais canais estão ocupados.

Para ilustrar melhor a aplicação do protocolo 802.22, a figura 1 faz uma comparação entre os diversos protocolos wireless. Tipicamente, é possível prover banda larga wireless para uma área rural entre 17-30 km entre uma antena externa do usuário e a estação base, sendo possível estender até a 100 km a uma velocidade de 1.5 Mbps.

Nos Estados Unidos, as estações de TV operam em 68 canais na porção VHF e UHF do espectro de rádio. Esses canais possuem largura de banda de 6 MHz, sendo alocados em diversas faixas entre 54 e 806 MHz.

Embora a maior demanda comercial de implementação do RC esteja vindo dos EUA, o 802.22 busca estender o alcance operacional de 41 a 910 MHz e acomodar também canais com largura de banda de 7 e 8 MHz, definindo assim um padrão internacional que opere nos diversos regimes regulatórios pelo mundo.

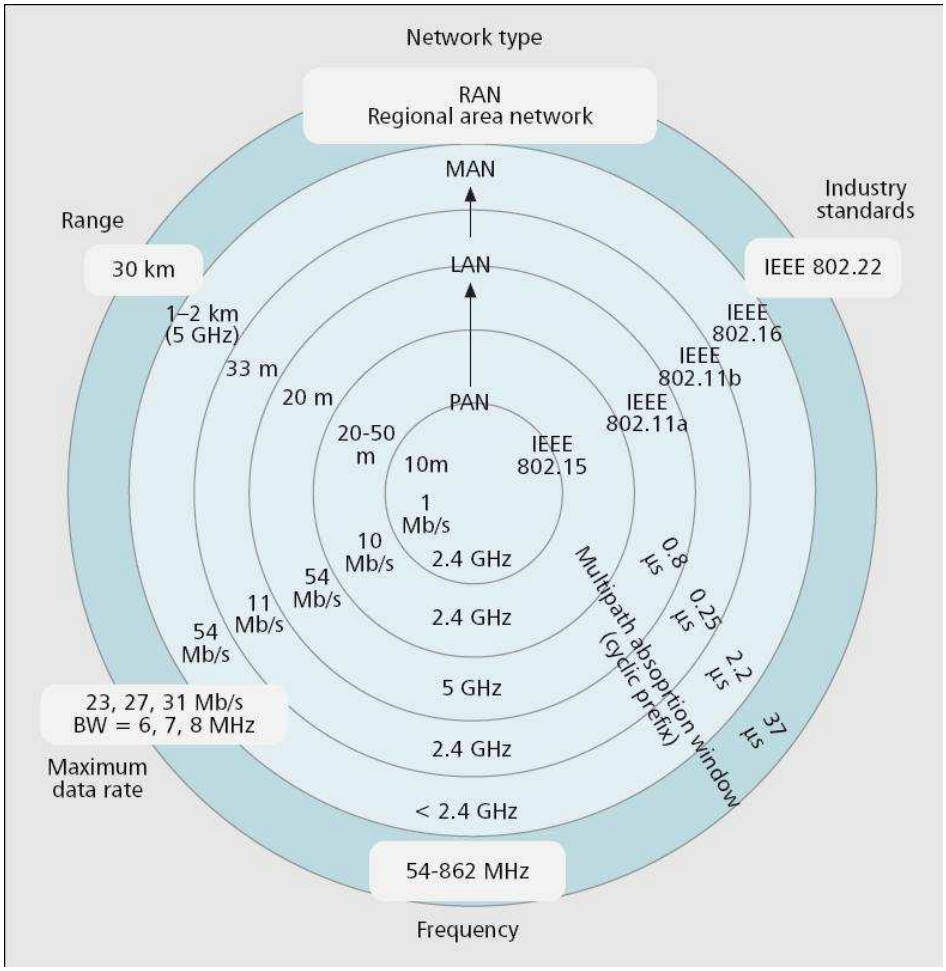


Figura 1 – Comparação do 802.22 wireless RAN em relação a outros padrões wireless

2.1 TOPOLOGIA E RELACIONAMENTOS

802.22 especifica um sistema ponto (fixo) – multiponto, em que uma estação base (BS) gerencia sua célula e suas estações cliente associadas. Essa estação base, além das funções tradicionais em redes wireless, também gerencia o processo distribuído de escuta ao meio. Isso é necessário para garantir a proteção dos usuários licenciados, uma vez que a BS irá instruir as estações cliente a realizar medições distribuídas em diversos canais de TV. Baseado na resposta desses clientes a BS irá decidir o próximo passo.

2.2 A CAMADA PHY

A camada PHY do protocolo implementa três funções: escuta do ambiente (espectro), geo-localização e comunicação de dados, sendo as duas primeiras responsáveis por prover as funcionalidades necessárias para suportar as habilidades cognitivas do sistema. Uma vez que os equipamentos dos usuários finais podem estar localizados a diferentes distâncias da estação base (BS) ou apresentando diferentes níveis de ruído, a BS deve ser capaz de ajustar dinamicamente banda, modulação e codificação. Esses requisitos são implementados na camada PHY.

O padrão implementa o processo de escuta em duas fases: uma primeira fase de escuta rápida do espectro (*fast sensing*) e a fase de escuta refinada (*fine sensing*). As medições realizadas na primeira fase servem para determinar a necessidade e a duração da fase de escuta refinada. A precisão das técnicas de escuta depende de fatores externos, como a presença de ruídos.

802.22 emprega um *framework* distribuído para escuta do espectro, em que qualquer nó que represente um cliente necessita reportar seus resultados à estação base. Usando esses resultados locais, a estação base ajusta os parâmetros da camada PHY, tais como largura de banda do canal, modulação ou taxa de codificação.

2.3 A CAMADA MAC

A camada MAC provê mecanismos para transmissão de dados eficiente e flexível protegendo transmissores primários licenciados e permitindo a coexistência entre os sistemas 802.22, sem depender dos parâmetros específicos de transmissão de cada país.

Diferentemente de outras tecnologias wireless, os procedimentos de inicialização na camada MAC não definem apenas processos de sincronização, negociação de capacidades, autorização, registro e configuração de conexão, mas também especificam explicitamente operações de geo-localização, acesso ao banco de dados de canais, escuta inicial do espectro e sincronização entre redes.

Basicamente, 802.22 emprega uma estrutura de superframes, ilustrada na figura 2. A estação base envia inicialmente um cabeçalho de controle do superframe (CCS) em frequências de canais de TV (máximo de 3) que podem ser utilizadas na comunicação. Estações Cliente (EC) que estejam sintonizadas em algum desses canais e que sincronizem e recebam esse cabeçalho, são capazes de obter as informações necessárias para se associar à BS. O superframe tem um tempo de vida e, durante esse tempo, múltiplos frames MAC podem ser transmitidos, utilizando múltiplos canais, provendo melhor capacidade do sistema e taxa de transmissão de dados.

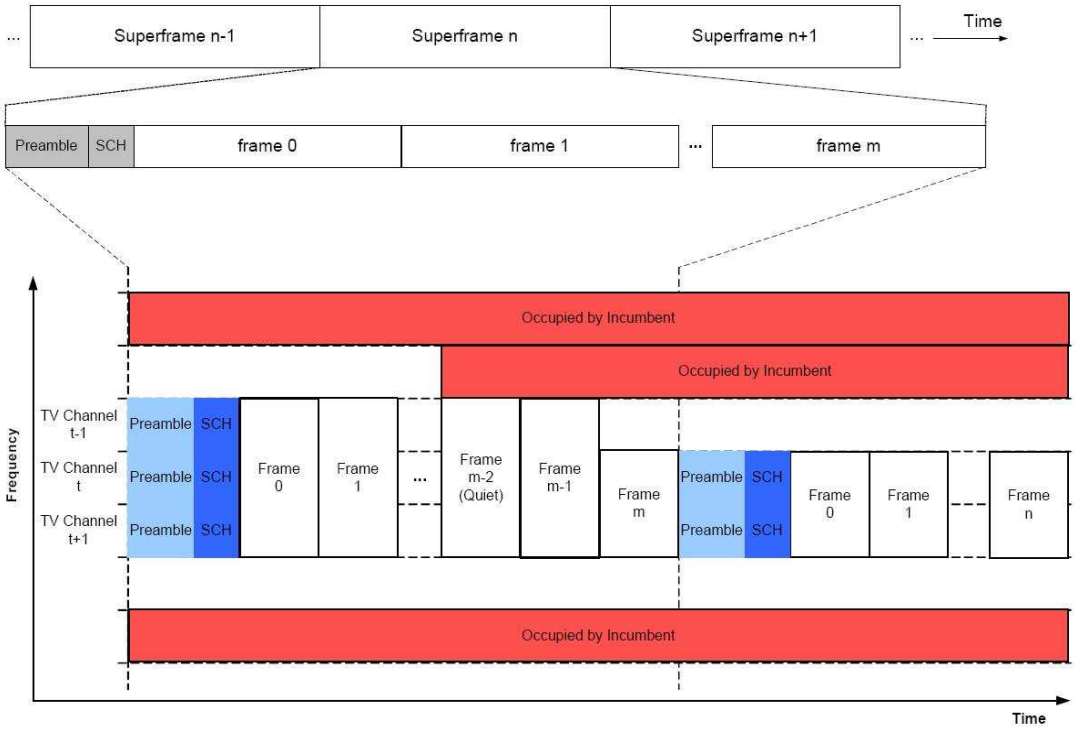


Figura 2 – Estrutura do Superframe

A estrutura de um frame MAC é formada por duas partes, conforme figura 3: um *downstream subframe* (DS) e um *upstream subframe* (US). O primeiro subframe consiste apenas de uma PDU PHY com um possível intervalo de contenção para fins de coexistência. O subframe US consiste de intervalos de contenção agendados para processos de inicialização, requisição de banda ou notificações.

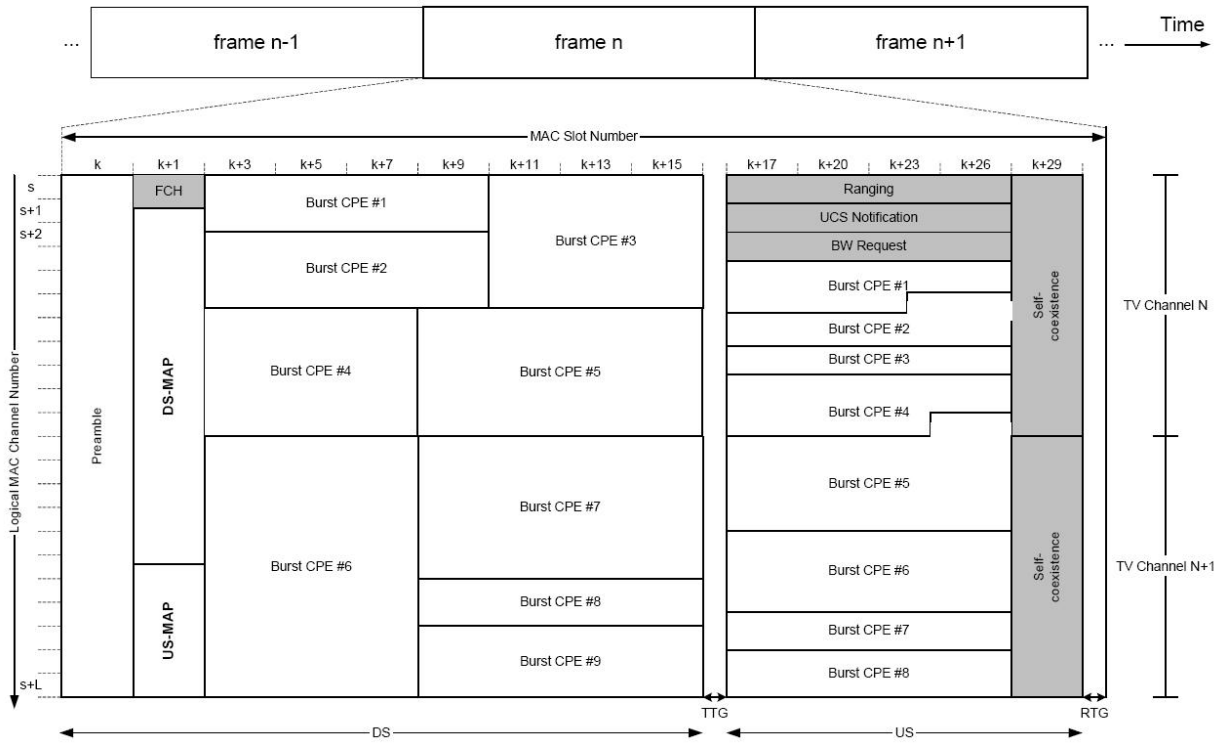


Figura 3 – Estrutura do superframe: tempo e frequência.

Ao contrário das tecnologias wireless tradicionais, não há um canal pré-determinado em que um equipamento cliente possa procurar por uma BS e realizar os procedimentos de inicialização na rede. Logo, este equipamento, quando for iniciado, deve realizar primeiramente um escaneamento dos canais de TV para montar um mapa de ocupação do espectro que identifique, para cada canal, se há equipamentos licenciados ativos.

Nos canais livres o equipamento do cliente deve escanear por transmissões de CCS (cabeçalho de controle do superframe) de uma BS, ficando em cada canal no mínimo pelo período de um superframe. Uma vez recebido o CCS, o canal e informações da rede já estão disponíveis para entrada e inicialização da rede.

Um dos principais componentes da camada MAC do 802.22 está relacionado às características cognitivas do protocolo: o gerenciamento de canais e medições do espectro. É função da BS instruir cada um de seus equipamentos 802.22 associados a realizar atividades de medição periódicas.

Dependendo dos algoritmos de detecção de uso do espectro usado por cada equipamento, as medições podem ter durações diferentes. Porém, a BS tem a função de indicar que canais cada equipamento deve medir e por quanto tempo. Com o objetivo de se obter um melhor desempenho, equipamentos não precisam necessariamente realizar as mesmas medições. Pode ser incorporado no sistema um algoritmo para distribuir as medições numa célula e assim obter um mapa geral de ocupação do espectro, sendo este retornado para a BS que tomará ações.

2.3.1 Compartilhamento de Bandas entre Estações Base

A troca de mensagens entre células (unidade controlada por uma estação base) é de vital importância, uma vez que podem estar sobrepostas e terem que compartilhar espectro. O padrão especifica dois tipos de sinalização entre células:

- *BS Beacons*: sinalização utilizada para prover informação sobre o agendamento de tráfego, canal de operação atual da célula, etc.
- *Clients Beacons*: sinalização utilizada para prover informação do nó cliente sobre a atual célula em que está operando e também informações sobre o fluxo de tráfego entre o nó e a sua BS.

Para facilitar a detecção de usuários primários, a BS periodicamente agenda um período de silêncio, se possível sincronizado com os períodos de silêncio das BS vizinhas. Nesse período todo tráfego de rede é suspenso para todas as entidades do sistema escutarem o espectro para detecção de usuários primários.

O SIR (Signal-to-Interference Ratio) é a razão entre a potência do sinal de interesse e a interferência total a que ele está sujeito. Neste caso a BS agenda suas transmissões de dados nesse canal com o controle de potência apropriado para não gerar interferência nas células vizinhas.

Toda célula requer certo número de canais para prover o nível adequado de QoS para as suas aplicações. Quando a condição atual dos canais não é suficiente para suportar o QoS previsto, a BS que está necessitando de mais espectro inicia um processo de compartilhamento dinâmico de recursos inter-BS em busca de mais canais livres ou de melhores canais. 802.22 prevê dois tipos de compartilhamento de recursos inter-BS: compartilhamento de espectro exclusivo e não exclusivo.

A escolha entre o compartilhamento exclusivo ou não exclusivo é realizada após a BS escolher um canal e utilizar o seguinte critério: se o máximo SIR alcançável no canal escolhido for maior que o limiar requerido para suportar os serviços da célula, é utilizado o compartilhamento não exclusivo.

2.4 A SUBCAMADA DE SEGURANÇA

A subcamada de segurança definida no IEEE 802.22 provê serviços de confidencialidade, autenticação e integridade dos dados, por meio da utilização de mecanismos criptográficos nas unidades de dados MAC que trafegam nas conexões entre clientes e BS. A subcamada de segurança possui dois componentes: um protocolo de encapsulamento e um protocolo PKM (Privacy Key Management). O

primeiro protocolo define um conjunto de mecanismos criptográficos suportados, como por exemplo, algoritmos de autenticação e as regras para aplicar esses algoritmos no *payload* da PDU da camada MAC (MPDU). O protocolo PKM garante a segurança na distribuição de chaves entre a BS e os clientes.

A subcamada de segurança protege as informações de controle da rede anexando MAC (Message Authentication Code) nas mensagens de gerenciamento da camada Cognitiva MAC. Porém, a subcamada de segurança protege apenas o tráfego interno da célula. O tráfego entre células não é protegido. Logo, sinalizações entre células são vulneráveis a modificações não autorizadas ou falsificação. A figura 4 ilustra o escopo de atuação da subcamada de segurança em relação às funcionalidades do protocolo 802.22.

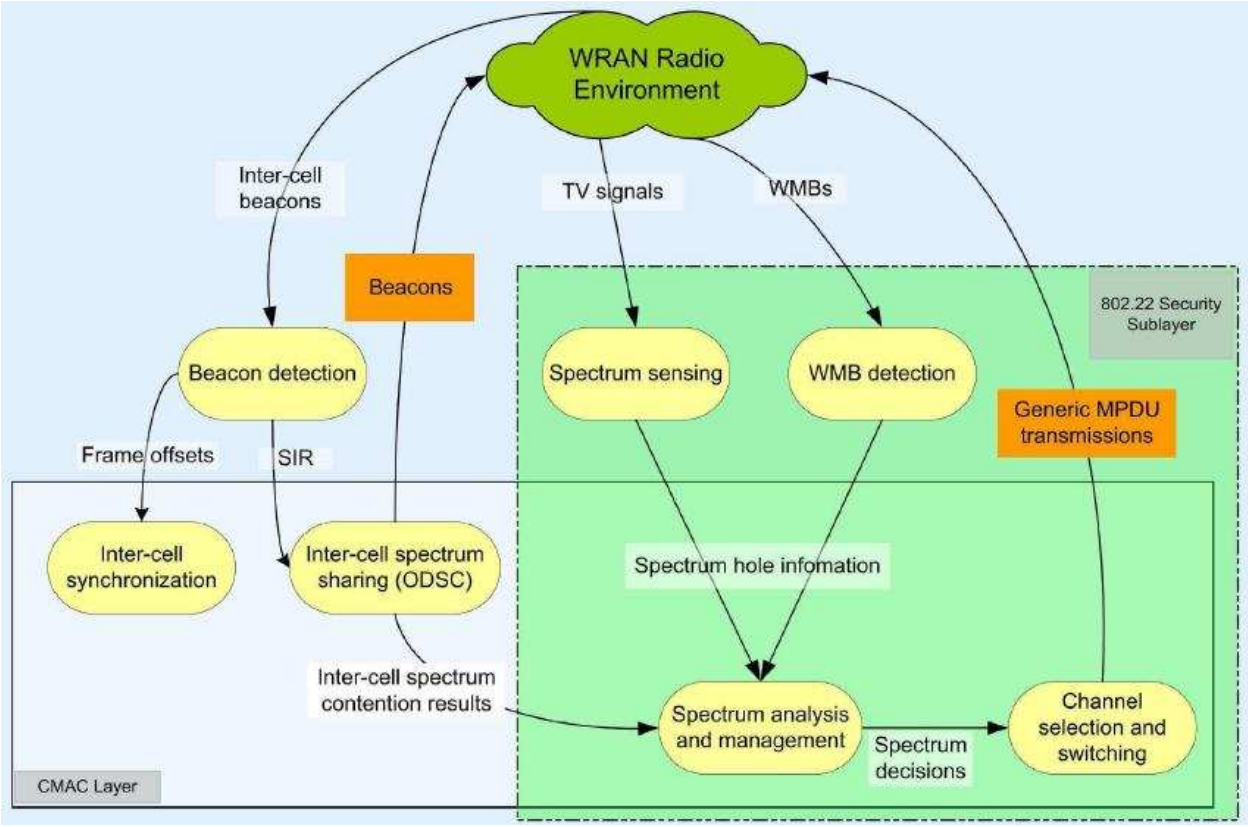


Figura 4 – Funcionalidades do protocolo 802.22 e o escopo da subcamada de segurança

3 CARACTERÍSTICAS DE RÁDIOS COGNITIVOS E DE REDES DE RÁDIOS COGNITIVOS

Ao se falar em RC eventualmente pode-se confundir com o termo *software radio* que é geralmente um rádio que suporta múltiplas interfaces e protocolos wireless e também opera em várias bandas, podendo ser reconfigurado por software ou até microprocessadores, de acordo uma política estabelecida. RC opera em cima de uma plataforma de rádio com certa “inteligência” para ser potencialmente capaz de reconfiguração autônoma através do aprendizado e adaptação do ambiente de comunicação.

Software radios normalmente possuem vários sensores que transformam a energia RF recebida em resultados quantitativos, como por exemplo: um detector pode medir a energia recebida numa determinada frequência com o objetivo de determinar se um canal está ocupado. Também possuem uma interface para compartilhar as opções de configuração e sensores para uma entidade controladora. Essa entidade precisa escolher um conjunto de entradas na configuração do *software radio* que resultem em resultados otimizados.

Para realizar essa otimização, a função cognitiva é introduzida. Todas essas entradas e resultados aparecem na base de conhecimento da função cognitiva como registros de estatísticas (somente leitura) e como registros de configuração (leitura e escrita). A base de conhecimentos é um conjunto de expressões lógicas que representam o estado do rádio.

Comparado com rádios tradicionais, RC possuem características especiais tais como inteligência artificial e uma aplicação de acesso ao espectro, descritas a seguir.

3.1 INTELIGÊNCIA ARTIFICIAL (IA)

RC oferece as capacidades de aprender e se adaptar ao ambiente através de métodos de aprendizado e raciocínio. A IA pode ser representada por um modelo de quatro componentes: observações, ações, rotinas de inferência e uma base de conhecimento. O aprendizado e raciocínio são resultado de uma operação combinada das rotinas de inferência e da base de conhecimentos.

Um rádio cognitivo requer políticas para lidar com diferentes ambientes e reagir a diferentes condições. Ou seja, as políticas são a base da característica de raciocínio do RC, que pode ser vista como um conjunto de regras lógicas de inferência. Nesse conjunto devem ser definidas as ações a serem tomadas, em que condições devem ser tomadas, e como essas ações afetarão a base de conhecimento. A limitação, porém, dessa característica de raciocínio é que ela necessita de políticas pré-programadas e não se adapta a novas situações.

Um rádio com funcionalidades de aprendizado pode ganhar experiência com estatísticas passadas e com a análise do ambiente atual para prever o ambiente futuro e selecionar as melhores ações. O modelo de aprendizado é um processo em que as rotinas de inferência avaliam relacionamentos, tais como ações executadas no passado ou observações atuais, e converte essas informações para a base de conhecimento. Essa funcionalidade de aprendizado permite ao RC se adaptar a diferentes situações e operar sem políticas pré-programadas.

Embora essas características permitam mais flexibilidade e desempenho, também expõem os RC a uma série de novas ameaças, descritas mais a frente.

Pode-se definir o ciclo cognitivo como sendo:

Observar ➔ Orientar ➔ Planejar ➔ Decidir ➔ Agir.

Sempre que este ciclo resultar num novo estado de operação, caso o rádio suporte aprendizado, um novo estado de aprendizado é injetado no ciclo, permitindo a adição de informação na memória sobre como o rádio fez a transição para esse novo estado. Essa informação pode ser usada para planejar e decidir em ciclos futuros. Caso o ataque seja realizado no estágio de observação todos os outros estágios serão influenciados. Em rádios baseados em políticas, manipulação do estágio de observação afetará o “Agir” durante apenas um ciclo cognitivo. Em rádios baseados em aprendizado, as consequências podem ter impacto a longo prazo.

3.2 ACESSO DINÂMICO AO ESPECTRO (ADE)

Como exposto anteriormente, o espectro de frequências é regulado por agências governamentais e atribuídos a usuários licenciados, e para largas regiões geográficas. O aumento de dispositivos wireless fez com que o espectro de frequências se tornasse um recurso escasso. Pesquisas realizadas pela FCC (Federal Communications Commission) sobre a utilização do espectro, apontaram uma variação de 15 a 85% tendo como base a localização geográfica e o uso no tempo. O uso de ADE foi uma solução encontrada para aumentar a eficiência da utilização do espectro, permitindo o uso de bandas licenciadas por usuários não licenciados de modo “oportunístico”.

O acesso dinâmico ao espectro é constituído basicamente de quatro funções: escuta do meio; gerenciamento (escolha do melhor canal disponível); mobilidade (manter a comunicação durante a transição de espectro); e compartilhamento de canais (coexistência com outros usuários em um canal).

Uma rede de rádios cognitivos (RRC) é um conjunto de nós RC que interagem uns com outros para dinamicamente se adaptar às variações das

condições da rede. RRCs podem ser classificadas de três formas, de acordo com as soluções existentes de compartilhamento de espectro:

- Arquitetura de rede: centralizada ou distribuída. No primeiro caso existe uma entidade central que controla a alocação de espectro e procedimentos de acesso. Outros nós são responsáveis por encaminhar suas medições e informações para a unidade central. Numa arquitetura distribuída cada nó é responsável pela alocação de espectro e o acesso é baseado em políticas locais.
- Comportamento dos nós: cooperação ou sem cooperação. Soluções de cooperação consideram o efeito da comunicação de um nó com outros da rede. Todas as soluções centralizadas podem ser vistas como soluções de cooperação. Também existem soluções de cooperação distribuídas.
- Tecnologia de acesso: *overlay* ou *underlay*. A tecnologia baseada em *overlay* acessa o espectro que não está sendo usado no momento por usuários licenciados, minimizando assim a possibilidade de interferência na comunicação desses usuários. Já o *underlay* opera na faixa de ruído dos usuários primários, ou seja, na porção do espectro que é considerada ruído para usuários licenciados.

4 AMEAÇAS DE SEGURANÇA A REDES DE RÁDIOS COGNITIVOS

A técnica de rádio cognitivo é a técnica chave para implementar uma política de acesso dinâmico ao espectro de frequência. Contudo, assim como várias outras técnicas, fatores de segurança são deixados fora de foco, no período de inicialização. Comparado com rádios tradicionais, RC são mais flexíveis e mais expostos a ameaças de segurança.

Ameaças de segurança típicas em redes wireless normalmente são mitigadas adicionando ao sistema mecanismos de autenticação e criptografia. Tais mecanismos normalmente funcionam bem para garantir a confidencialidade dos dados que atravessam a rede sem fio, porém, não obrigatoriamente garantem o bom funcionamento da comunicação.

4.1 AMEAÇAS RELATIVAS À INTELIGÊNCIA ARTIFICIAL

Podem ser identificadas algumas classes mais comuns de ameaças de segurança a rádios cognitivos ou redes de rádios cognitivos. A primeira delas são as que atacam as características de inteligência artificial.

4.1.1 Ataque às Políticas

O RC necessita de políticas para operar apropriadamente em diferentes condições. Políticas são inseridas no rádio no momento da fabricação e podem ser atualizadas ou estendidas durante o uso através de transferências entre os RC e do recebimento de políticas anunciadas localmente ou distribuídas com um período de validade. Como pode ser observado, existem várias maneiras de se receber políticas e, por outro lado, negar o recebimento de políticas pode afetar a qualidade da comunicação. Fica claro que uma ameaça pode reduzir a efetividade da

comunicação bloqueando o acesso às políticas ou interferindo na transmissão do rádio que as transmite.

Dentro dos problemas de segurança relacionados a políticas, podem ser destacados os ataques de modificação e o uso de falsas de políticas. No primeiro caso uma ameaça pode invadir um RC ou um banco de dados de políticas e modificá-las. Também há o caso de um host malicioso injetar falsas políticas no momento em que o RC está atualizando seu banco de dados através de sinalização de rádio das políticas locais. Em ambos os casos, caso o RC opere segundo a falsa política, pode ser gerada interferência na transmissão em rádios licenciados ou mesmo em outros RC da rede.

4.1.2 Ataques ao Processo de Aprendizado

Numa rede de rádios cognitivos (RC), alguns nós são designados para ter a capacidade de aprendizado, podendo aprender de experiências passadas ou de situações atuais para prever o ambiente futuro, e assim poder selecionar os melhores modos de operação. Essa característica, porém, também pode ser alvo de ataque. Estatísticas passadas podem ser modificadas assim como o ambiente atual pode ser falsificado, comprometendo a previsão do ambiente futuro (figura 5). Esse tipo de ataque é de difícil detecção e pode ocasionar efeitos indesejados a longo prazo.

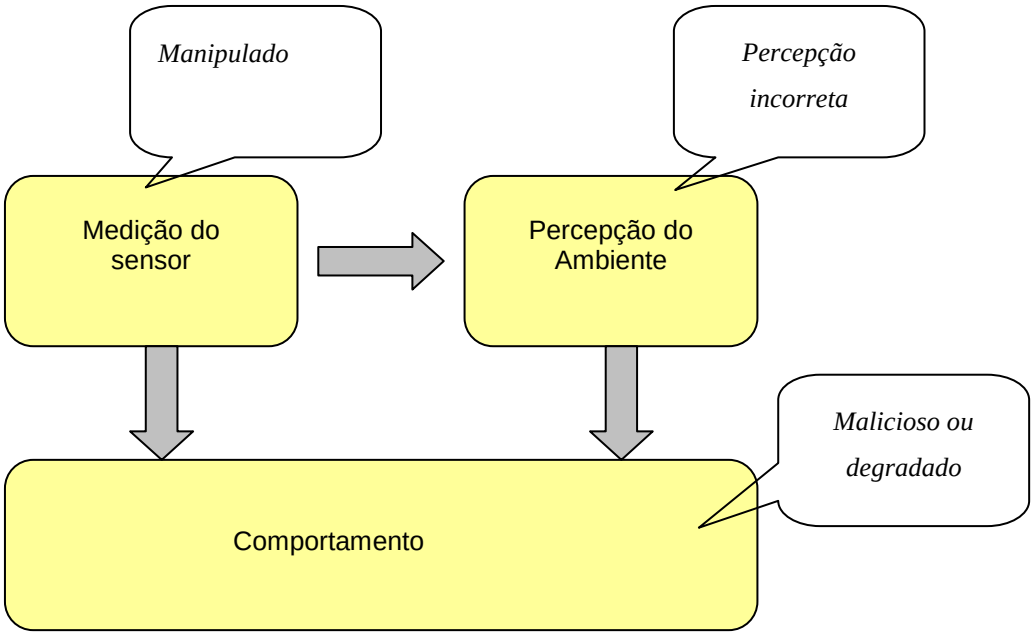


Figura 5 – Relacionamento entre a medição do sensor e o comportamento futuro do RC, numa situação em que os dados de entrada do sensor estão sendo manipulados.

Um exemplo prático é o método de aprendizado através da cadeia de Marcov, que considera que uma faixa do espectro é dividida em N canais, alocados para usuários licenciados, que de acordo com as estatísticas de tráfego pode ser classificados em dois estados: ocupado e ocioso. A longo prazo, os RC podem ter uma previsão da ocupação futura dos canais. Porém, em caso de modificação dos dados de entrada da cadeia de Marcov, ou seja, do estado dos canais, os RC podem ficar esperando o canal ficar ocioso mesmo ele já estando ou, por outro lado, começar a transmitir quando o canal estiver ocupado, gerando interferência em usuários primários.

4.1.3 Alteração dos Parâmetros de Configuração

Outra modalidade de ataque relevante é a alteração de parâmetros de operação dos RC. Funções cognitivas manipulam esses parâmetros com o tempo para maximizar sua performance. Alguns parâmetros possíveis de entrada são: largura de banda, frequência, tipo de modulação, tipo de criptografia, tamanho do frame, energia, codificação ou protocolo de acesso ao canal.

É definida uma função que objetiva basicamente três itens: potência de transmissão, taxa de transmissão e segurança. Dependendo da aplicação, pode ser dado peso diferente para cada um desses objetivos. Por exemplo, em um sistema que roda aplicações de emails, segurança deveria ter peso maior do que taxa de transmissão. Em aplicações de áudio e vídeo, taxa de transmissão deve ter um peso alto.

Existem vários tipos de ataque em sistemas deste tipo. Quando os rádios estão na fase de aprendizado, eles tentam diversas combinações de parâmetros de entrada, medem as estatísticas observadas, tal como taxa de erros, e avaliam a função para ver quais dados de entrada dão melhores resultados para uma dada aplicação.

Dos três objetivos, potência, taxa de transmissão e segurança, apenas o segundo é afetado pelo canal. Potência e segurança são definidos diretamente pelos parâmetros de entrada enquanto a taxa de transmissão é definida pelas saídas do sistema. Logo, afetando o canal de comunicação, altas taxas de transmissão podem não ser alcançadas.

4.2 ACESSO DINÂMICO AO ESPECTRO

A segunda classe de ameaças a ser definida são as que afetam o Acesso Dinâmico ao Espectro (ADE). Podem ser relativas ao processo de escuta, ao gerenciamento do espectro ou relativas às características de mobilidade do protocolo.

4.2.1 Ameaças Relativas ao Processo de Escuta do Ambiente

Rádios cognitivos, por serem usuários secundários do espectro, devem usar o espectro oportunisticamente, quando não houver transmissão de nenhum usuário licenciado (primário). Para isso é necessário que os RC possuam algoritmos capazes de detectar brechas na utilização do espectro e, adicionalmente, para liberar o canal sempre que um usuário primário iniciar uma transmissão. Usuários secundários também podem ter que compartilhar a banda com outro usuário secundário, na ausência de melhores bandas.

É muito difícil para um nó da rede, por si só, ter um conhecimento preciso do mapa de ocupação do espectro. Logo há a necessidade dos RC realizarem uma comunicação entre si de forma a cada nó ter uma cooperação na escuta do espectro local e enviar para os outros. Essa comunicação distribuída se dá via um canal de controle comum. Percebe-se que deve haver confiabilidade nas identidades e informações enviadas por cada nó da rede para garantir resultados corretos após a fusão das coletas locais.

A partir do momento que o resultado das escutas individuais é compartilhado no canal de controle, é requerido alto nível de segurança nesse canal, como por exemplo, autenticação das transações entre os nós.

Uma das ameaças consiste em realizar um *spoof* da identidade do usuário primário. Nesse caso o host que vai realizar o ataque simula uma transmissão num canal e o usuário secundário que estiver transmitindo no momento irá interromper a transmissão, acreditando ser uma transmissão de um usuário licenciado. Esse ataque é conhecido como Primary User Emulation – PUE ou Emulação do Usuário Primário. Após o ataque, o atacante fica livre para utilizar o espectro. Esse ataque, porém, não gera efeitos a longo prazo, já que no momento em que o atacante liberar o canal ou parar de emular a transmissão, o usuário secundário detectará o canal livre e poderá iniciar a transmissão.

Há também outro tipo de ataque que bloqueia o recebimento de informações dos sensores dos RC sobre a ocupação do meio por usuários primários. Como explicado acima, em alguns RC as informações dos sensores são transmitidas por um canal de controle, sendo fácil para hosts maliciosos gerar interferência. Existe o caso em que o sensor e o rádio compartilham a mesma interface, porém, mesmo que sejam separados, a operação do sensor pode ser deteriorada pela transmissão do rádio. Logo a escuta do meio e transmissão não podem ocorrer ao mesmo tempo, sendo dedicada uma fração do tempo para a transmissão e outra para a escuta. Interferência durante o tempo de escuta pode gerar sérios impactos na comunicação. Para diminuir a influência da interferência, recomenda-se reservar a fração do tempo dedicada à transmissão o mais próximo possível de 100%, o que vai requerer melhores algoritmos de escuta.

Replay attacks: um ataque comum utilizado por hosts maliciosos é o de capturar mensagens locais de escuta do ambiente enviadas dos clientes para a estação base e enviá-las novamente, ocasionando percepção incorreta da BS sobre o ambiente. IEEE 802.22 impede esse tipo de ataque de repetição de pacotes de

dados utilizando o protocolo de criptografia AES em modo combinado com autenticação de mensagens (para garantir autenticidade dos dados).

Como o rádio cognitivo não está utilizando apenas suas próprias observações para utilizar como base para as suas decisões, mas também dados enviados por outros, é obvio que há a necessidade de autenticar as observações compartilhadas no canal de controle. Além da garantia da autenticidade do remetente da mensagem, é importante o rádio cognitivo ter a habilidade de julgar se as observações reportadas são reais ou falsificadas.

Resumindo, para mitigar ataques maliciosos ao processo de escuta, que levam os RC a terem um comportamento forçado, o sistema deve possuir as seguintes características: habilidade de autenticar as observações locais; habilidade de trocar informações seguramente com outros elementos da rede; habilidade de julgar as observações reportadas; e habilidade de realizar uma análise do próprio comportamento.

4.2.2 Ameaças Relativas ao Processo de Gerenciamento do Espectro

Após a escuta do ambiente, os RC detectam as bandas ociosas do espectro para comunicação, bandas essas que apresentam diferentes características em relação à largura, frequência de operação, etc. O RC deve ter a capacidade de selecionar a banda do espectro mais apropriada para os usuários, baseando-se para tal em requisitos de QoS e características do espectro.

As funções do processo de gerenciamento podem ser classificadas em análise e decisão o espectro. A primeira consiste na caracterização de diferentes bandas enquanto a segunda seleciona a banda apropriada para a transmissão atual, considerando os requisitos de QoS.

Nesse caso, as ameaças consistem na possibilidade de falsas características do espectro serem analisadas, podendo resultar na escolha de uma banda inapropriada para a transmissão. Métodos de estimativa da capacidade do espectro consideram fatores como a largura da banda, ruídos ou potência do sinal. Caso atacantes consigam alterar algum desses fatores, a análise do espectro ficará comprometida.

4.2.3 Ameaças Relativas às Características de Mobilidade

A característica de mobilidade visa garantir que a comunicação não será afetada quando um RC saltar de um canal para outro, devido à ocupação da banda por um usuário primário ou devido à movimentação do rádio, por exemplo. Para isso, o RC precisa selecionar e se mover imediatamente para outra banda apropriada (*handoff*).

Esse período de *handoff* é susceptível a várias ameaças, uma vez que um *handoff* falho resulta num longo período de tempo para restabelecer a comunicação. Nesse caso, um host atacante pode obrigar o RC a liberar o canal, emulando um host primário, e depois gerar interferência para atrasar ou causar falhas no processo de seleção de uma nova banda disponível.

4.3 AMEAÇAS EM REDES DE RÁDIOS COGNITIVOS

A terceira classe de ameaças tem como objetivo redes de rádios cognitivos (RRC). Como já explicado anteriormente, há três tipos de classificação para as RRC: centralizadas ou distribuídas; cooperação ou sem cooperação; e *underlay* e *overlay*. A arquitetura centralizada e com cooperação são mais vulneráveis aos ataques, já que, no caso da entidade central ser manipulada ou sofrer um ataques de DoS, toda

a rede fica comprometida. Numa rede com cooperação, se um dos nós for manipulado por um atacante, este pode transmitir falsas informações para os outros. Em redes distribuídas e sem cooperação esse tipo de ataque não afeta os outros nós, uma vez que todos operam independentemente.

Em relação ao uso das tecnologias de *overlay* e *underlay*, no primeiro caso a rede está sujeita a ataques de emulação do usuário primário para evitar que o RC detecte banda disponível e assim não consiga transmitir. No caso do uso de *underlay*, é relativamente fácil fazer com que um CR comprometido possa gerar interferência em usuários primários.

Como já mencionado no item 2.4, a versão atual do 802.22 não especifica mecanismos eficientes de segurança para mensagens de sinalização entre células. Logo, todas as mensagens de controle entre elas estão sujeitas a ataques do tipo modificação não autorizada, falsificação ou *replay*. Esse fato se dá pelo atual protocolo ter herdado a maior parte das características da subcamada de segurança do protocolo 802.16 – WI-MAX, que não considera em sua implementação a necessidade de tratamento de usuários primários e da coexistência com outros usuários secundários.

Devido a essa vulnerabilidade nos mecanismos de sinalização entre células são identificados dois tipos de ataques: interrupção do processo de disputa de espectro e interferência do processo de sincronização entre células. Em ambos os casos o atacante manipula as mensagens de sinalização, o que pode ser conseguido, por exemplo, pela manipulação do software do RC.

4.3.1 Ataque ao Processo de Disputa do Espectro

Para realizar esse tipo de ataque, um terminal sob controle de um atacante primeiramente escolhe um canal que esteja sendo utilizado numa célula (a vítima), através de escuta das mensagens de sinalização da BS vítima. Depois o atacante envia mensagens espúrias requisitando espectro, via mensagens forjadas de sinalização entre células. A célula vítima é acionada para participar da disputa pelo espectro e caso perca, ela libera o canal de operação atual tendo que procurar outro.

Caso o atacante inicie muitos processos de disputa de espectro e ganhe a maior parte dessas disputas, a célula vítima pode perder uma parte significante dos seus recursos de rede, ocasionando uma degradação do desempenho. Deve ser observado que é obtido efeito similar caso um nó malicioso capture mensagens de disputa de espectro e execute subsequente *replay*.

A efetividade desse ataque aumenta significantemente se as mensagens forjadas forem enviadas no período de escuta da célula vítima, pois há maior chance da mensagem ser recebida. Isso significa que a efetividade do ataque aumenta se as transmissões do atacante estiverem sincronizadas com a das vítimas.

4.3.2 Interferência do Processo de Sincronização de Células

Segundo o padrão 802.22, células sobrepostas devem sincronizar seus períodos de escuta do meio sempre que possível para aumentar a precisão do processo de escuta do meio. Como dito anteriormente, não existem mecanismos capazes de garantir a segurança da sinalização entre células. Então, a partir do momento em que células vizinhas coordenam a sincronização, a partir da troca

dessas mensagens de sinalização, já estão sujeitas a ataques de falsificação de mensagens.

Caso um host envie uma sinalização para células vizinhas inserindo *offsets* falsos dos frames, resultará numa sincronização errada e uma medição imprecisa das condições do meio, já que os usuários dessa célula terão que escutar a transmissão de usuários primários durante o período de transmissão de dados da rede.

5 ESTRATÉGIAS DE MITIGAÇÃO DAS VULNERABILIDADES E AMEAÇAS

Face às ameaças e vulnerabilidades apresentadas, diversas soluções foram apresentadas para tentar mitigar os diversos ataques a que rádios cognitivos estão expostos. Nesse capítulo serão apresentados algumas alternativas de solução, bem como suas vantagens e limitações.

5.1 ASSINATURAS DIGITAIS PARA REDES CENTRALIZADAS

Nos capítulos anteriores foi citada a existência de um ataque simples, porém com graves efeitos para os RC, que era um DoS através da emulação da identidade do usuário primário. Esse ataque se baseia na inabilidade de usuários secundários de distinguir as transmissões de usuários primários e usuários maliciosos. A solução proposta baseia-se na identificação do usuário utilizando-se algoritmos de criptografia de chave pública.

Nesse esquema, qualquer algoritmo de criptografia pública pode ser utilizado, sendo identificadas basicamente quatro entidades participantes: os usuários primários, uma autoridade certificadora, a estação base de uma célula e os usuários secundários dessa célula.

Embora algoritmos de chaves públicas possam ser utilizados para garantir confidencialidade dos dados, nessa solução serão usados apenas como assinatura digital para garantir autenticidade dos usuários primários. O processo de assinatura consiste na criptografia de uma mensagem com a chave privada de um usuário a que se queira confirmar como autor, e apenas a chave pública correspondente conseguirá decifrar corretamente essa mensagem.

Ao usuário primário deve ser atribuído um par de chaves pública/privada, assinadas pela autoridade certificadora (CA) correspondente. A CA é uma entidade

central à rede que, além de assinar as chaves dos usuários, é responsável por manter e disponibilizar as chaves públicas dela mesma e dos usuários para futura verificação das assinaturas ou criptografia de dados em sistemas que requeiram confidencialidade.

Nesse caso, o usuário primário assina com sua chave privada os campos Identidade (PID) e Time Stamp, contidos no cabeçalho MAC de cada MPDU, e concatena o resultado na transmissão após cada MPDU.

A verificação da assinatura pelos usuários secundários é feita durante o período de escuta refinada (*fine sensing*). Caso seja detectada a presença de um usuário primário, o dispositivo secundário decodifica o sinal para obter as MPDUs. Se for encontrada alguma assinatura, ela é separada da MPDU e armazenada pelo usuário secundário e, periodicamente, as assinaturas armazenadas são transmitidas para a estação base por um canal de controle.

A estação base obtém da CA, por uma conexão segura, uma lista com as identidades dos usuários primários e as respectivas chaves públicas. Uma vez recebidas as assinaturas dos usuários secundários, a BS armazena uma cópia delas e decodifica com cada uma das chaves públicas dos usuários primários. Se a identidade obtida após a decodificação com uma das chaves for igual a uma das identidades dos usuários primários da lista, a BS checa a validade do *time stamp*. Para isso, a BS seleciona um parâmetro de *delay*, X, que define uma faixa de *time stamp* aceitável. Se a diferença absoluta entre a hora atual da BS e o *time stamp* decriptografado for igual ou menor que X, a presença de um usuário primário é garantida. O valor de X, entretanto, deve ser escolhido de forma que a assinatura não “expire” antes de ser decriptografada pela BS.

A segurança desse esquema está diretamente relacionada com a impossibilidade de se forjar uma assinatura digital. Um dos ataques comuns, o *replay attack*, em que um atacante captura uma assinatura válida e retransmite, também é mitigado, uma vez que o *time stamp* é incluído na assinatura e ela não pode ser utilizada fora da faixa determinada por X. Logo, X não pode ser muito pequeno de forma que a assinatura expire e também não pode ser muito grande de forma a possibilitar ataques do tipo *replay*.

A segurança da CA também é fator crucial para o funcionamento do sistema, uma vez que, caso seja comprometida e as chaves modificadas, os usuários primários podem nunca ser reconhecidos, gerando interferência constante aos receptores primários. A transmissão entre a CA e as demais entidades deve ser segura.

Pode-se observar que a BS tem participação importante na confirmação das identidades dos usuários primários. O esquema de identificação, porém, pode exaurir os recursos da BS, principalmente se hosts maliciosos transmitirem assinaturas randômicas em grande quantidade. O mecanismo de descartar assinaturas duplicadas reduz esse problema, porém não o elimina completamente. O fato do esquema proposto também não assinar a MPDU inteira, e sim apenas a Identidade e o *time stamp*, faz com que o esquema seja computacionalmente mais leve.

Por outro lado, o esquema apresentado possui uma série de limitações, uma delas relativas aos usuários primários que transmitem sinais analógicos, como é o caso de muitos transmissores de TV. Nesse caso, as primitivas criptográficas não podem ser empregadas. Existem formas de se identificar uma transmissão analógica

de um usuário primário através de suas características criptográficas, porém, não se garante que elas não serão imitadas.

Outra grande limitação da solução reside em ambientes descentralizados. Como visto anteriormente, há a necessidade de uma entidade central no sistema que esteja ao alcance de todos os usuários, para assumir a responsabilidade de autoridade certificadora.

5.2 FRAMEWORK PARA SEGURANÇA NO CANAL DE CONTROLE

Dentre as muitas funções providas pela camada MAC do rádio cognitivo, pode-se destacar a de estabelecer o canal de controle para que os RC possam trocar informações sobre os canais. O canal de controle está sujeito a uma série de ameaças, como descrito em capítulos anteriores, sendo parte crítica para o bom funcionamento de uma rede de RC. A solução a seguir, tem o objetivo de garantir confiabilidade entre as partes envolvidas nas trocas de informação e garantir que os nós de uma rede, mesmo que descentralizada, não gerem interferência entre si e nem em usuários primários.

Numa rede distribuída onde os nós trabalham em cooperação não existe uma estação base para centralizar a comunicação, logo a negociação de canal deve ser feita entre cada par de RC. Durante essa negociação, frames MAC como a Lista de Canais Livres (FCL), Seleção de Canal (CH-SEL) e Reserva de Canal (CH-RES) são utilizados entre as entidades envolvidas.

O primeiro mecanismo de defesa é a autenticação entre os nós, que pode ser obtida por meio de algoritmos de chave pública/privada, seguidos de troca de chave secreta para garantir confidencialidade nas fases seguintes da negociação.

Adicionalmente, a integridade das mensagens trocadas pode ser obtida utilizando-se Message Authentication Code ou *hash*.

A seleção do canal é realizada logo após as operações de autenticação, por meio das trocas dos frames FCL, CH-SEL e CH-RES, conforme figura 6. Após um nó enviar a lista de canais livres, o receptor seleciona um canal livre comum aos dois e, posteriormente, o primeiro nó envia uma confirmação.

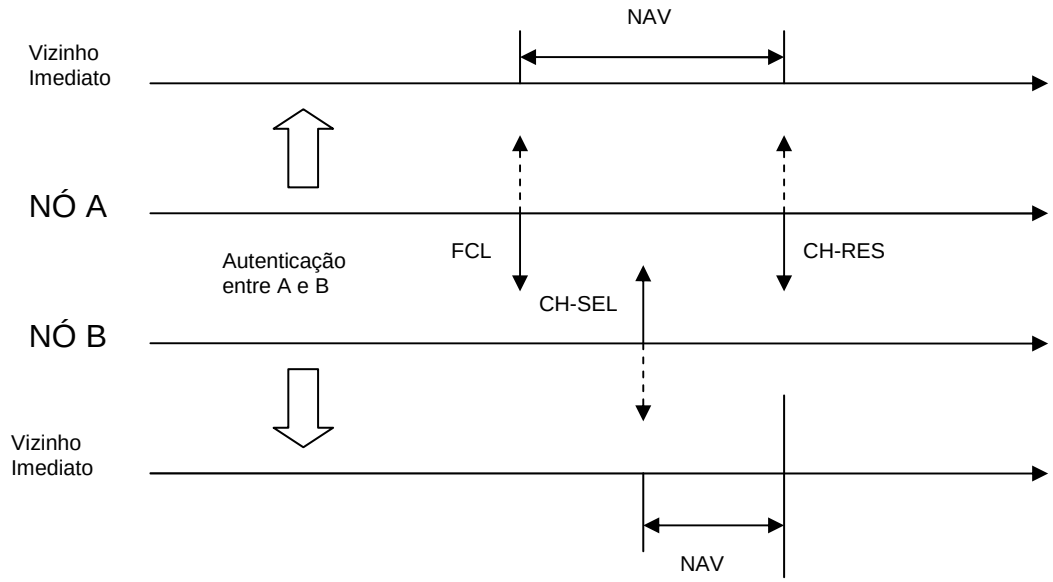


Figura 6 – Negociação de canal num ambiente distribuído.

É importante observar que, nos períodos identificados por NAV (Network Allocation Vector), os nós vizinhos imediatos param de transmitir, para evitar interferência.

A autenticação também é realizada com os nós vizinhos imediatos, que também recebem uma cópia da chave de sessão, usada para garantir a confidencialidade da negociação de canais. O conhecimento da chave de sessão

possibilita aos nós vizinhos conhecer o canal reservado e evitá-lo, atualizando a sua FCL. Essa lista de canais livres é então repassada aos vizinhos mais distantes.

A solução apresentada, porém, continua sujeita a ataques de DoS em que um usuário malicioso gera interferência no canal de controle e inviabiliza a comunicação entre as entidades da rede.

5.3 PROCEDIMENTO PARA VERIFICAÇÃO DO TRANSMISSOR

A solução apresentada a seguir tem o objetivo de mitigar os ataques de Emulação do Usuário Primário, utilizando-se de procedimentos de verificação do transmissor que podem ser integrados ao mecanismo de escuta do espectro. O procedimento é baseado na verificação da localização do transmissor para distinguir o usuário primário de um sinal não licenciado mascarado.

A tarefa de distinguir sinais de usuários primários e secundários torna-se mais difícil devido ao requisito imposto pela própria FCC de que o acesso oportunístico ao espectro deve ser realizado sem que haja qualquer obrigação dos usuários primários de fazerem modificações em seus sistemas. Por essa razão, abordagens como a de incorporar assinaturas digitais no sinal do usuário licenciado ou o emprego de um protocolo interativo entre as partes, não pode ser usada.

A verificação é executada por entidades previamente designadas como verificadores de localização (VL) que, passivamente, escutam o sinal sem interagir com o transmissor. O esquema de verificação é baseado em duas técnicas: o Teste de Distância do Rádio (TDR) e o Teste de Diferença de Distâncias (TDD). O primeiro utiliza as medições de potência do sinal, obtidas de um par de VL para verificar a localização do transmissor. O segundo verifica a diferença da fase do sinal em questão nos dois VL.

Porém, para o esquema funcionar, uma série de premissas deve ser garantida: o modelo trata de transmissores primários de TV fixos e necessita da presença de dois VL dedicados, podendo ser uma estação base ou um usuário secundário, para realizarem TDR e TDD. Os VL devem possuir um banco de dados com as coordenadas de todas as torres de TV, cujo sinal alcança a rede cognitiva em questão. Assume-se também que torres de TV normalmente possuem potência da ordem de grandeza de centenas ou milhares de watts, enquanto usuários secundários operam na faixa de centenas de miliwatts.

Baseado nas premissas acima, pode-se assumir que se a origem do sinal for muito diferente das localizações das torres de TV contidas no banco de dados, então há possibilidade de estar ocorrendo um ataque de emulação do usuário primário. Um atacante, contudo, pode estar transmitindo nas vizinhanças de uma torre de TV, não sendo possível detectar o ataque apenas pela localização da origem do sinal. Nesse caso, a potência do sinal recebido também é analisada, uma vez que a magnitude do sinal de um usuário secundário é bem menor do que de uma torre de TV.

O detalhamento das técnicas utilizadas para realizar os testes de localização e nível de energia, TDR e TDD, não são o foco dessa pesquisa, porém observa-se a necessidade de haver um canal de controle seguro para comunicação dos VL, e que também existe a possibilidade de um atacante posicionar estrategicamente seus transmissores para contornar o procedimento de verificação da localização, caso conheça a posição dos VL. Uma contramedida para tal ataque é o uso de VL escondidos, conhecidos apenas pela autoridade que controla o processo de verificação de localização. O canal de controle, deve ser criptografado e autenticado para evitar ataques do tipo modificação, escuta ou ataques de *replay*.

6 CONCLUSÃO

Pode-se considerar que rádio cognitivo ainda está num estágio precoce de desenvolvimento, sendo necessário considerar os fatores de segurança na arquitetura das aplicações. Nessa pesquisa, foram descritas características especiais de RC e redes de RC, como por exemplo, inteligência artificial, acesso dinâmico ao espectro e os três tipos de classificação que podem ser feitas em relação ao modo de funcionamento de redes de RC.

Após, ameaças de segurança e vulnerabilidades devido à essas características foram mencionadas em detalhes, sendo seguidas de contramedidas e aspectos chaves que devem ser observados.

Ainda há muitas questões de segurança não resolvidas para redes de rádios cognitivos, especialmente considerando as limitações requeridas pela FCC dos usuários primários não serem obrigados a serem modificados para permitir o acesso oportunístico ao espectro pelos usuários secundários. Algumas delas são listadas a seguir:

- Técnicas mais avançadas de identificação do transmissor. Foram explanados alguns mecanismos de autenticação do sinal para identificação do usuário primário, porém, o uso de características não forjáveis do usuário licenciado é requerido.
- Uso de mecanismos de proteção para evitar ataques referentes às mensagens se sinalização entre estações base vizinhas, prejudicando o processo de escuta do meio e consequentemente obtendo uma leitura errada das condições do meio, conforme 4.3.2.

- Mecanismos para detectar e excluir nós maliciosos internos. Para isso, é necessário identificar operação anormal do nó através da análise do tráfego e cooperação entre os outros nós da rede.
- Desenvolvimento de mecanismos eficientes de gerenciamento do espectro, baseados em políticas, de modo a permitir à rede de RC ser dinamicamente configurada, devido à alta taxa de variação das condições da rede. As políticas devem incluir controle de admissão, usando, por exemplo, 802.1x e gerenciamento de identidade.
- Integração da informação de todos os usuários secundários da vizinhança para obter-se uma correta decisão em relação ao uso do espectro, mesmo com a presença de um certo número de nós maliciosos.

7 REFERÊNCIAS

[1] SILVA, MARCEL WILLIAM ROCHA DA, RESENDE, JOSÉ FERREIRA DE, **Roteamento em Redes em Malha Híbridas de Rádios Cognitivos e IEEE 802.11.** XXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2009.

[2] BURBANK, J.L., **Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security**, Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on Publication Year: 2008 , Page(s): 1 - 7

[3] YUAN ZHANG, GAOCHAO XU, XIAOZHONG GENG, **Security Threats in Cognitive Radio Networks**, High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on, Publication Year: 2008 , Page(s): 1036 – 1041.

[4] CLANCY, T.C.; GOERGEN, N., **Security in Cognitive Radio Networks: Threats and Mitigation**, Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on, Publication Year: 2008 , Page(s): 1 - 8

[5] RUILIANG CHEN; JUNG-MIN PARK; HOU, Y.T.; REED, J.H., **Toward secure distributed spectrum sensing in cognitive radio networks**, Communications Magazine, IEEE Volume: 46 , Issue: 4 Publication Year: 2008 , Page(s): 50 - 55

[6] PRASAD, N.R., **Secure Cognitive Networks**, Wireless Technology, 2008. EuWiT 2008. European Conference on, Publication Year: 2008 , Page(s): 107 - 110

[7] SAFDAR, G.A.; O'NEILL, M., **Common Control Channel Security Framework for Cognitive Radio Networks**, Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th, Publication Year: 2009 , Page(s): 1 - 5

[8] SHAUKAT, R.; KHAN, S.A.; AHMED, A., **Augmented Security in IEEE 802.22 MAC Layer Protocol**, Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, Publication Year: 2008 , Page(s): 1 - 4

[9] CORDEIRO, CARLOS; CHALLAPALI, KIRAN; BIRRU, DAGNACHEW, **IEEE 802.22: An Introduction to the first Wireless Standard based on Cognitive Radios**, Journal of Communications, Vol1, No 1, Publication Year: 2006, Page(s): 38 - 47

[10] S. ARKOULIS. L. KAZATZOPOULOS. C. DELAKOURIDIS. G.F. MARIAS., **Cognitive Spectrum and its Security Issues**, Proceedings of the 2008 The

Second International Conference on Next Generation Mobile Applications, Services, and Technologies, Pages: 565-570, Year of Publication: 2008

[11] KAIGUI BIAN, JUNG-MIN "JERRY" PARK, **Security Vulnerabilities in IEEE 802.22**, ACM International Conference Proceeding Series, Proceedings of the 4th Annual International Conference on Wireless Internet, SESSION: Cognitive radio networks, Article No.: 9, Year of Publication: 2008

[12] MATHUR, CHETAN N., SUBBALAKSHMI, K. P., **Digital Signatures for Centralized DSA Networks**, 4th IEEE Consumer Communication and Networking Conference. Publication Year: 2007, Page(s): 1037 – 1041

[13] CHEN, R., PARK, J., **Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks**. SDR '06. 1st IEEE Workshop on. Publication Year: 2006, Page(s): 110 - 119

[14] LEÓN, O., HERNÁNDEZ-SERRANO, J., SORIANO, M., **Securing Cognitive Radio Networks**, International Journal of Communication Systems, Volume 23 Issue 5, Pages 633 – 652, Published Online: 10 Feb 2010